CLAIMS

(65)

1. A safety verification device of a reactive system represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a set of terms to be verified,

said set of axioms being a set consisting only a commutative law and an associative law, and

said safety verification device of a reactive system comprising:

a translation unit generating, under said set of axioms, a first equational tree automaton which accepts said set of terms,

a simulation unit generating, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set comprising terms derived from said set of terms, and

a set operation unit which generates a fourth equational tree automaton by associating said second equational tree automaton with a third equational tree automaton which accepts said set of terms to be verified and determines whether or not a set accepted by the fourth equational tree automaton is an empty set.

2. A safety verification device of a reactive system represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a term to be verified,

said set of axioms being a set consisting only a commutative law and an associative law, and

said safety verification device of a reactive system comprising:

a translation unit generating, under said set of axioms, a first equational tree automaton which accepts said set of terms,

a simulation unit generating, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational

tree automaton which accepts said set of terms and a set comprising terms derived from said set of terms, and

a set operation unit determining whether or not said second equational tree automaton accepts said term to be verified.

3. A safety verification device of a reactive system according to claim 1 or 2, wherein said set of function symbols is a set comprising function symbols representing encryption, decryption and communication processing as elements,

said set of rewriting rules is a set comprising as an element a rule representing that encrypted information is returned to plaintext by decryption,

said term to be verified is confidential information, and

said set of terms is a set of knowledge of each of subjects that exchange confidential information, and a set of knowledge of a subject that monitors the information exchanged between said subjects.

4. A safety verification method of a reactive system represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a set of terms to be verified,

said set of axioms being a set consisting only a commutative law and an associative law, and

said method comprising:

a first step of generating, under said set of axioms, a first equational tree automaton which accepts said set of terms,

a second step of generating, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms derived from said set of terms, and

a third step of generating a fourth equational tree automaton by associating said second equational tree automaton

with a third equational tree automaton which accepts said set of terms to be verified and determining whether or not a set accepted by the fourth equational tree automaton is an empty set.

5. A safety verification method of a reactive system represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a term to be verified,

said set of axioms being a set consisting only a commutative law and an associative law, and

said method comprising:

a first step of generating, under said set of axioms, a first equational tree automaton which accepts said set of terms,

a second step of generating, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms derived from said set of terms, and

a third step of determining whether or not said second equational tree automaton accepts said term to be verified.

6. A safety verification method of a reactive system according to claim 4 or 5, wherein said set of function symbols is a set comprising function symbols representing encryption, decryption and communication processing as elements,

said set of rewriting rules is a set comprising as an element a rule representing that encrypted information is returned to plaintext by decryption,

said term to be verified is confidential information, and

said set of terms is a set of knowledge of each of subjects that exchange confidential information, and a set of knowledge of a subject that monitors the information exchanged between said subjects.

7. A computer-readable recording medium containing a

reactive system safety verification computer program, comprising:

a first program code which accepts an input of a procedure represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a set of terms to be verified,

a second program code which generates, under said set of axioms consisting only of a commutative law and an associative law, a first equational tree automaton which accepts said set of terms,

a third program code which generates, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms derived from said set of terms, and

a fourth program code which generates a fourth equational tree automaton by associating said second equational tree automaton with a third equational tree automaton which accepts said set of terms to be verified and determines whether or not a set accepted by the fourth equational tree automaton is an empty set.

8. A computer-readable recording medium containing a safety verification computer program, comprising:

a first program code which accepts an input of a procedure represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a term to be verified,

a second program code which generates, under said set of axioms consisting only of a commutative law and an associative law, a first equational tree automaton which accepts said set of terms,

a third program code which generates, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms

derived from said set of terms, and

a fourth program code which determines whether or not said second equational tree automaton accepts said term to be verified.

9. A computer-readable recording medium containing a reactive system safety verification computer program according to claim 7 or 8, wherein said set of function symbols is a set comprising function symbols representing encryption, decryption and communication processing as elements,

said set of rewriting rules is a set comprising as an element a rule representing that encrypted information is returned to plaintext by decryption,

said term to be verified is confidential information, and

said set of terms is a set of knowledge of each of subjects that exchange confidential information, and a set of knowledge of a subject that monitors the information exchanged between said subjects.

10. A computer program data signal embodied in a carrier wave for reactive system safety verification, comprising:

a first program code which accepts an input of a procedure represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a set of terms to be verified,

a second program code which generates, under said set of axioms consisting only of a commutative law and an associative law, a first equational tree automaton which accepts said set of terms,

a third program code which generates, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms derived from said set of terms, and

a fourth program code which generates a fourth equational tree automaton by associating said second equational tree automaton with a third equational tree automaton which accepts said set of terms to be verified and determines whether or not a set accepted by the fourth equational tree automaton is an empty set.

11. A computer program data signal embodied in a carrier wave for reactive system safety verification, comprising:

a first program code which accepts an input of a procedure represented by a set of function symbols, a set of rewriting rules, a set of axioms, a set of terms, and a term to be verified,

a second program code which generates, under said set of axioms consisting only of a commutative law and an associative law, a first equational tree automaton which accepts said set of terms,

a third program code which generates, under said set of rewriting rules and said set of axioms and using said first equational tree automaton as initial data, a second equational tree automaton which accepts said set of terms and a set of terms derived from said set of terms, and

a fourth program code which determines whether or not said second equational tree automaton accepts said term to be verified.

12. A computer program data signal embodied in a carrier wave for reactive system safety verification according to claim 10 or 11, wherein said set of function symbols is a set comprising function symbols representing encryption, decryption and communication processing as elements,

said set of rewriting rules is a set comprising as an element a rule representing that encrypted information is returned to plaintext by decryption,

said term to be verified is confidential information,

and

said set of terms is a set of knowledge of each of subjects that exchange confidential information, and a set of knowledge of a subject that monitors the information exchanged between said subjects.